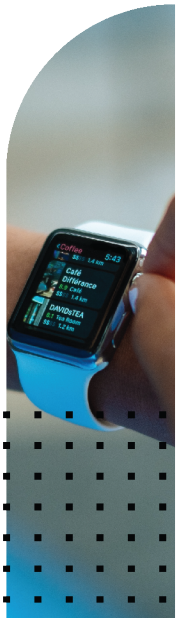
Release Notes

FortiAuthenticator 6.3.0



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

June 3, 2021
FortiAuthenticator 6.3.0 Release Notes
23-630-713057-20210603

TABLE OF CONTENTS

Change log

Date	Change Description
2021-04-22	Initial release.
2021-04-27	Updated What's new on page 8
2021-04-28	Added new feature Logging: Ability to send FortiAuthenticator debug logs to remote logging servers to What's new on page 8.
2021-06-03	Added new feature Captive portal: Support for Cisco WLC to What's new on page 8.

FortiAuthenticator 6.3.0 release

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, and resolved and known issues for FortiAuthenticator 6.3.0, build 0670.

FortiAuthenticator is a user and identity management solution that provides strong authentication, wireless 802.1X authentication, certificate management, RADIUS AAA (authentication, authorization, and accounting), and Fortinet Single Sign-On (FSSO).

For additional documentation, please visit: https://docs.fortinet.com/product/fortiauthenticator/

Special notices

TFTP boot firmware upgrade process

Upgrading FortiAuthenticator firmware by interrupting the FortiAuthenticator boot process and installing a firmware image from a TFTP server erases the current FortiAuthenticator configuration and replaces it with factory default settings.

Monitor settings for GUI access

Fortinet recommends setting your monitor to a screen resolution of 1600x1200. This allows for all the objects in the GUI to be viewed properly without the need for scrolling.

Before any firmware upgrade

Save a copy of your FortiAuthenticator configuration before upgrading the firmware. From the administrator dropdown menu in the toolbar, go to **Restore/Backup**, and click **Download Backup File** to backup the configuration.

After any firmware upgrade

Clear your browser cache before logging in to the FortiAuthenticator GUI to ensure the pages display properly.

What's new

FortiAuthenticator version 6.3.0 includes the following new features and enhancements:

Enhancements to the FortiAuthenticator REST API

Various improvements and endpoints added to the FortiAuthenticator 6.3.0 REST API Solutions guide.

For more information, see the REST API Solutions Guide.

Exporting MAC devices list

You can now export the list of MAC devices configured in *Authentication* > *User Management* > *MAC Devices*.

FortiToken Mobile logo configuration

The FortiToken configuration page now includes a separate tab where users can upload logo images for their organization which are sent to the FortiToken Mobile app during provisioning. The FortiToken Mobile app displays this logo beside the one-time password for the specific token. This can be used to distinguish between tokens when there are multiple tokens managed by the same FortiToken Mobile app.

FortiToken Mobile logos can be configured by selecting the Logos tab now available in **Authentication > User Management > FortiTokens**.

This option replaces the previous **Organizations** page which included the same features, previously available in **Authentication > User Management > Organizations**.

Monitor active SAML IdP sessions

A monitor for viewing active SAML IdP sessions is available in **Monitor > Authentication > SAML IdP Sessions**. The page contains the following elements:

- A table containing the list of IdP sessions.
- Search options at the top of the table to search by username or by user IP address.
- The total number of SAML sessions.

TACACS+ Import clients through CSV file

TACACS+ clients can be imported and assigned to TACACS+ policies through a CSV file.

Sync rule: Import RADIUS users from LDAP server

You can now configure a remote LDAP user synchronization rule that allows you to create, edit, or delete remote RADIUS users. When this synchronization rule runs, it creates remote RADIUS users available in **User Management > Remote Users**.

FortiToken Mobile push notification contains user IP and geolocation

FortiAuthenticator now shows user IP and/or geolocation in the FortiToken mobile push notifications in the following locations when available:

- A new **Look up geo-location of user IP for Web Service** toggle in **Authentication > User Account Policies > General**.
- A new **Application name for FTM push notification** field when creating or editing a SAML Service Provider in **Authentication > SAML IdP > Service Providers**.
- A new **Application name for FTM push notification** field and **Resolve user geolocation from their IP address** toggle when creating or editing a self-service portal policy in **Authentication > Portals > Policies**.
- A new **Application name for FTM push notification** field and **Resolve user geolocation from their IP address** toggle when creating or editing a captive portal policy in **Authentication > Portals > Policies**.
- A new **Application name for FTM push notification** field and **Resolve user geolocation from their IP address** toggle when creating or editing a RADIUS policy in **Authentication > RADIUS Service > Policies**. RADIUS policies also contain a new **RADIUS attribute for user IP** field that allows you to specify the RADIUS attribute to obtain the user IP from.

RADIUS Attributes and Certificate Bindings available to users with administrator or sponsor role

RADIUS Attributes and **Certificate Bindings** tabs are available when you create, edit, or import a user with the role as **Administrator** or **Sponsor** in the following locations:

- **Authentication > User Management > Local Users**.
- **Authentication > User Management > Remote Users**: RADIUS attributes and certificate bindings are available when you import an LDAP user.

  Only **Certificate Bindings** tab is available for RADIUS users, and SAML users do not have these tabs.

When creating, editing, or importing a user with its role as **Administrator** or **Sponsor**, this feature is available only if **Sync in HA Load Balancing mode** is enabled.

GUI: Improved LDAP group selection UX

The new **Set Group Filter** button in **Create New Remote LDAP User Synchronization** window allows you to set the LDAP filter by selecting one or more groups to build the LDAP filter string in **Authentication > User Management > Remote User Sync Rules**.

The **Set Group Filter** button is also available for the LDAP user groups.

Captive portal: Support for Cisco WLC

FortiAuthenticator captive portal now supports Cisco WLC devices. It recognizes and handles redirects from a Cisco WLC device.

When configuring a captive portal policy in **Authentication > Portals > Policies**, FortiAuthenticator offers the following new built-in HTTP parameters when you select **Add Condition** in **Portal selection criteria > Additional source criteria**:

- **client_mac**
- **redirect_url**
- **switch_url**
- **wlan**

The **switch_url** HTTP parameter helps recognize a Cisco WLC captive portal redirect. After the user has successfully logged in to the FortiAuthenticator captive portal, FortiAuthenticator redirects the end user to the Cisco WLC API specified in the **switch_url** parameter.

Understanding the captive portal workflow help in the **Portal selection criteria** tab offers a new **Cisco WLC** topic in the **Access point/NAS** dropdown.

The **Authentication factors** tab has a new tooltip for **MAC address parameter** that lists which MAC parameter to use with a device type.

Symmetric encryption keys for debug logs and config files

When creating a configuration backup, the administrator has the option to enable or disable encryption, and specify the encryption password. By default, encryption is disabled.

When restoring a configuration backup, the administrator enters the decryption password if encryption is enabled. By default, decryption is disabled.

SAML IdP: IAM users

FortiAuthenticator now supports configuring IAM users and accounts in **Authentication > User Management > IAM**.

A new **IAM login** setting in **Authentication > SAML IdP > General** that allows IAM logins. When enabled, the SAML IdP login page shows a new **Sign-In as IAM user** link. This link takes you to the new customizable **IAM login** page.

Also, when you create an assertion attribute for a SAML service provider in **Authentication > SAML IdP > Service Providers**, it has the following new user attributes:

- **IAM account name**
- **IAM account alias**
- **IAM username**

A new **IAM** option when creating a local user that allows you to add this local user to an IAM account.

A new **Sync users to IAM Account** option when creating a remote LDAP user synchronization rule that allows you to synchronize the remote users with an IAM account.

A new **IAM Account** dropdown when importing SSO users in **Fortinet SSO Methods > SSO > SSO Users** that allows associating the imported users with an IAM account.

A new **SAML IdP Password Change Page** replacement message that allows customization of the password change page for a local user.

On successful IdP login of an IAM user associated with a local user for which **Force password change on next logon** is enabled, FortiAuthenticator presents a password change page same as the one for non-IAM local users.

New `iamaccounts` and `iamusers` endpoints available. A new `change_password` field is now available for the `localusers` endpoint.

For information about the new endpoints, see the REST API Solutions Guide.

SAML IdP: Support authentication from external IdP servers

FortiAuthenticator now supports IdP initiated SAML from the remote SAML IdP using an existing SAML IdP proxy server type.

The following new changes were implemented to support IdP initiated SAML:

- A new customizable **SAML IdP Proxy Login Success** page replacement message for successful IdP initiated login from a proxy remote SAML server.
- A new **Realm** user attribute is available when you create an assertion attribute for a SAML service provider in **Authentication > SAML IdP > Service Providers**. This new SAML assertion returns the realm that the end user was authenticated against.

The end user accesses the FortiAuthenticator SP login portal URL before the FortiAuthenticator IdP login page. From the SP login portal URL, the FortiAuthenticator determines the remote SAML server and identifies its associated realm.

Logging: Improvements for SIEM security analysis

The SAML IdP logs now include a new `userip` field that contains the end user IP address. Also, the `nas` field in the logs contains the name of the service provider.

To view log messages, go to **Logging > Log Access > Logs**.

SAML IdP: RADIUS attributes for assertions

FortiAuthenticator can now include attributes returned by the remote RADIUS servers into assertions returned by the SAML IdP.

There is a new option in the GUI to configure a SAML assertion containing the value of a RADIUS attribute:

- A new **RADIUS attribute** user attribute is available when you create an assertion attribute for a SAML service provider in **Authentication > SAML IdP > Service Providers**.

Captive portal: Support for WeChat social login

Captive portal in FortiAuthenticator now supports social login through WeChat.

Also, WeChat is now an option in the **Guest Portal Social Network Page** and **Guest Portal Social Network Plus FAC accounts** replacement messages in **Authentication > Portals > Replacement Messages**.

Adaptive Authentication

FortiAuthenticator now supports bypassing the OTP verification when the end user IP is on a trusted subnet for the following services:

- RADIUS authentication- A new **Adaptive Authentication** toggle available when creating or editing a RADIUS policy in **Authentication > RADIUS Service > Policies**.
- Captive portals- A new **Adaptive Authentication** toggle available when creating or editing a captive portal policy in **Authentication > Portals > Policies**.
- Self-service portals- A new **Adaptive Authentication** toggle available when creating or editing a self-service portal policy in **Authentication > Portals > Policies**.
- TACACS+ policies- A new **Adaptive Authentication** toggle available when creating or editing a TACACS+ policy in **Authentication > TACACS+ Service > Policies**.
- SAML IdP- In **Authentication > SAML IdP > Service Providers**, the **Bypass FortiToken authentication when user is from a trusted subnet** toggle is renamed to **Adaptive Authentication**.

TACACS+: Support for log files of size up to 500 MB

TACACS+ audit logs support a maximum file size of 500 MB. The following new size options are available:

- 100 MB
- 250 MB
- 500 MB

Certificates: GUI improvements

FortiAuthenticator now offers an improved GUI for the **Enrollment Requests** tab in **Certificate Management > SCEP**.

A new **Delete & Revoke Certificate** button in the **Enrollment Requests** tab that removes the selected SCEP enrollment request and revokes all the corresponding active user certificates. This option is available only if the **Automatic request type** for the selected request is **Regular**.

New tooltips for the **Subject** and the **Issuer** columns display the full subject and the issuer names.

FortiAuthenticator Agent for Microsoft OWA: Supports SMS, Email, and FTM push methods for 2FA

FortiAuthenticator Agent for Microsoft OWA supports SMS, Email, and FTM push methods for 2FA.

See *FortiAuthenticator Agent for Microsoft OWA 2.2 Release Notes* on the Fortinet Docs Library.

Group memberships when importing local users from a CSV file

You can now set group memberships when importing local users from a CSV file.

To support this feature, a new **group names** field is available in the CSV format.

When exporting the local users CSV file, FortiAuthenticator includes the list of local groups each user is a member of. When importing the local users CSV file, FortiAuthenticator adds the users to the specified groups.

FortiAuthenticator 800F and 300F support user license upgrades

You can now load an add-on user license to FortiAuthenticator 300F and 800F hardware models. This allows for better sizing flexibility without the need to maintain a wider number of different hardware models.

Similar to FortiAuthenticator-VM, **number of additional users** in the license specifies the number of additional users allowed on top of the built-in user limit. For example, if a license file with a FortiAuthenticator-300F serial number

specifies 1000 additional users, uploading that license onto the FortiAuthenticator-300F will result in a maximum user limit of 2500 (1500 built-in + 1000 license).

FSSO: Retry failed DNS lookups

Enable DNS lookup to get IP from workstation name available when the DC/TS Agent Clients setting is enabled in **Fortinet SSO Methods > SSO > General** allows FortiAuthenticator to retry DNS lookup to obtain the workstation IP address when the logon request contains only the workstation name.

If the initial lookup fails, FortiAuthenticator retries every 10 seconds for the following 5 minutes.

VM: Support disk partition increase

FortiAuthenticator now supports increasing the disk partition size when more disk space is allocated to a FortiAuthenticator-VM.

To allocate more disk space to the VM, use the `execute expand-partition` command in the CLI console. FortiAuthenticator reboots with an increased disk partition size.

In FortiAuthenticator 6.3.0, the maximum allowed disk size is 2 TB when attempting to increase the disk partition size.

Logging: Ability to send FortiAuthenticator debug logs to remote logging servers

FortiAuthenticator now supports sending debug logs to remote logging servers.

There is a new **Send debug logs to remote Syslog servers** toggle in **Logging > Log Config > Log Settings**.

Upgrade instructions

Back up your configuration before beginning this procedure. While no data loss should occur if the procedures below are correctly followed, it is recommended a full backup is made before proceeding and the user will be prompted to do so as part of the upgrade process.

For information on how to back up the FortiAuthenticator configuration, see the FortiAuthenticator Administration Guide.

Hardware and VM support

FortiAuthenticator 6.3.0 supports:

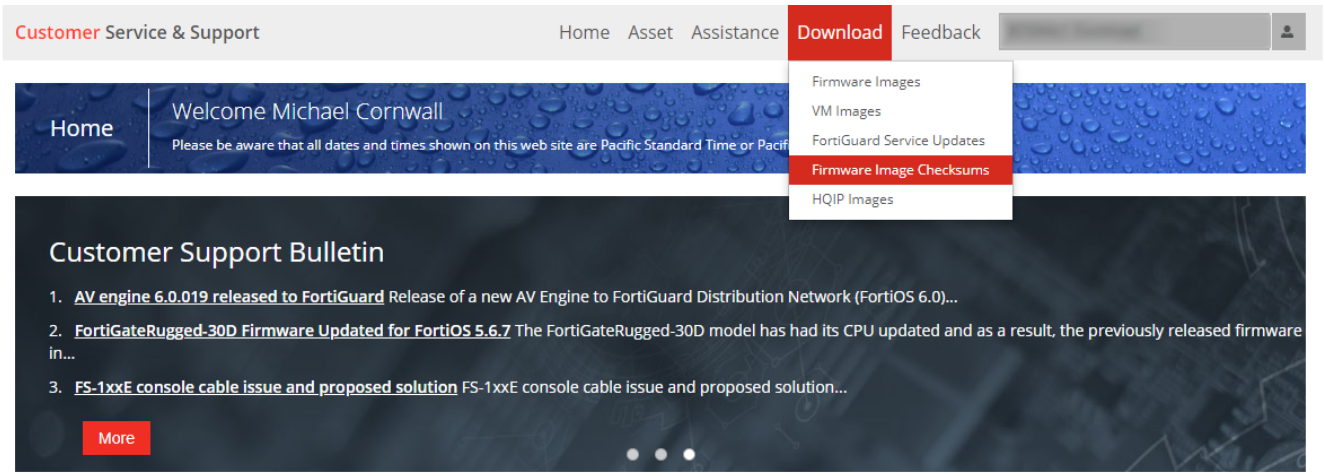
- FortiAuthenticator 200D
- FortiAuthenticator 200E
- FortiAuthenticator 400C
- FortiAuthenticator 400E
- FortiAuthenticator 1000D
- FortiAuthenticator 2000E
- FortiAuthenticator 3000D
- FortiAuthenticator 3000E
- FortiAuthenticator 800F
- FortiAuthenticator VM (VMWare, Hyper-V, KVM, Xen, Azure, AWS, Oracle OCI, and Alibaba Cloud)

Image checksums

To verify the integrity of the firmware file, use a checksum tool to compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for software releases are available from the Fortinet Support website.

Customer service and support image checksum tool



After logging in to the web site, in the menus at the top of the page, click **Download**, then click **Firmware Image Checksums**.

In the **Image File Name** field, enter the firmware image file name including its extension, then click **Get Checksum Code**.

Upgrading from FortiAuthenticator 4.x/5.x/6.x

FortiAuthenticator 6.3.0 build 0670 officially supports upgrade from FortiAuthenticator 6.0.4 and higher.

All other versions of FortiAuthenticator must first be upgraded to 6.0.4 or above before upgrading to 6.3.0, otherwise the following message will be displayed: `Image validation failed: The firmware image model number is different from the appliance's.`

When upgrading existing **KVM** and **Xen** virtual machines to FortiAuthenticator 6.3.0 from FortiAuthenticator 6.0.4, you must first increase the size of the virtual hard disk drive containing the operating system image (not applicable for AWS & OCI Cloud Marketplace upgrades). See Upgrading KVM / Xen virtual machines on page 17.

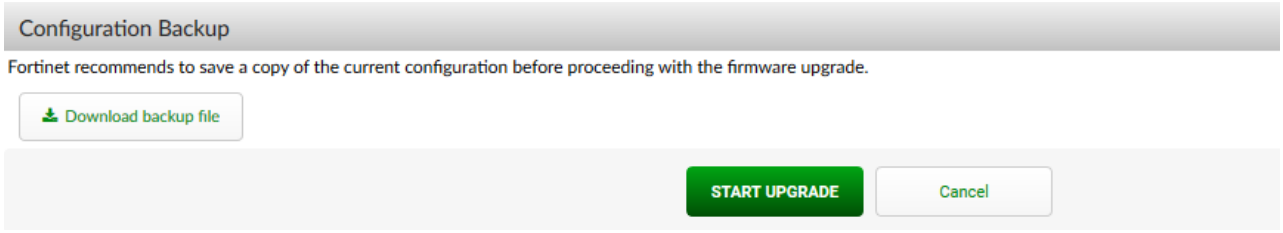
Firmware upgrade process

First, back up your configuration, then follow the procedure below to upgrade the firmware.

Before you can install FortiAuthenticator firmware, you must download the firmware image from the Fortinet Support website, then upload it from your computer to the FortiAuthenticator unit.

1. Log in to the Fortinet Support website. In the **Download** section of the page, select the **Firmware Images** link to download the firmware.
2. To verify the integrity of the download, go back to the **Download** section of the login page and click the **Firmware Image Checksums** link.
3. Log in to the FortiAuthenticator unit's web-based manager using the **admin** administrator account.

4. Upload the firmware and begin the upgrade.
   When upgrading from FortiAuthenticator 6.0.4 and earlier:
   a. Go to **System > Dashboard > Status**.
   b. In the **System Information** widget, in the **Firmware Version** row, select **Upgrade**. The **Firmware Upgrade or Downgrade** dialog box opens.
   c. In the **Firmware** section, select **Choose File**, and locate the upgrade package that you downloaded.
   When upgrading from FortiAuthenticator 6.1.0 or later.
   a. Click on the administrator name in the upper-right corner of the GUI to display the dropdown menu, and click **Upgrade**.
   b. In the **Firmware Upgrade or Downgrade** section, select **Upload a file**, and locate the upgrade package that you downloaded.
5. Select **OK** to upload the file to the FortiAuthenticator.
   Your browser uploads the firmware file. The time required varies by the size of the file and the speed of your network connection. When the file transfer is complete, the following message is shown:



   It is recommended that a system backup is taken at this point. Once complete, click **Start Upgrade**.
   Wait until the unpacking, upgrade, and reboot process completes (usually 3-5 minutes), then refresh the page.

Due to a known issue in 6.0.x and earlier releases, the port5 and port6 fiber ports are inverted in the GUI for FAC-3000E models (i.e. port5 in the GUI corresponds to the physical port6 and vice-versa).

This is resolved in 6.1.0 and later, however, the upgrade process does not swap these configurations automatically. If these ports are used in your configuration during the upgrade from 6.0.x to 6.1.0 and later, you will need to physically swap the port5 and port6 fibers to avoid inverting your connections following the upgrade.

Upgrading KVM / Xen virtual machines

When upgrading existing KVM and Xen virtual machines from FortiAuthenticator 6.0.4 to 6.3.0, it is necessary to manually increase the size of the virtual hard disk drive which contains the operating system image before starting the upgrade. This requires file system write-access to the virtual machine disk drives, and must be performed while the virtual machines are in an offline state, fully powered down.

If your virtual machine has snapshots, the resize commands detailed below will exit with an error. You must delete the snapshots in order to perform this resize operation. Please make a separate copy of the virtual disk drives before deleting snapshots to ensure you have the ability to rollback.

Use the following command to run the resize on KVM:

```
qemu-img resize /path/to/fackvm.qcow2 1G
```

Use the following command to run the resize on Xen:

```
qemu-img resize /path/to/facxen.qcow2 1G
```

After this command has been completed, you may proceed with the upgrade from 6.0.4 to 6.3.0

Recovering improperly upgraded KVM / Xen virtual machines

If the upgrade was performed without completing the resize operation above, the virtual machine will fail to properly boot, instead displaying many **initd** error messages. If no snapshots are available, manual recovery is necessary.

To recover your virtual machine, you will need to replace the operating system disk with a good copy, which also requires write-access to the virtual hard disks in the file system while the virtual machines are in an offline state, fully powered down.

To recover an improperly upgraded KVM virtual machine:

1. Download the 6.0.4 GA ZIP archive for KVM, **FAC_VM_KVM-v6-build0059-FORTINET.out.kvm.zip**.
2. Extract the archive, then replace your virtual machine's **fackvm.qcow2** with the one from the archive.
3. Execute the following command:
   ```
   qemu-img resize /path/to/fackvm.qcow2 1G
   ```

To recover an improperly upgraded Xen virtual machine:

1. Download the 6.0.4 GA ZIP archive for Xen, **FAC_VM_XEN-v6-build0059-FORTINET.out.xen.zip**.
2. Extract the archive, then replace your virtual machine's **facxen.qcow2** with the one from the archive.
3. Execute the following command:
   ```
   qemu-img resize /path/to/facxen.qcow2 1G
   ```

Product integration and support

Web browser support

The following web browsers are supported by FortiAuthenticator 6.3.0:

- Microsoft Internet Explorer version 11
- Microsoft Edge version 89
- Mozilla Firefox version 88
- Google Chrome version 89

Other web browsers may function correctly, but are not supported by Fortinet.

FortiOS support

FortiAuthenticator 6.3.0 supports the following FortiOS versions:

- FortiOS v7.0.x
- FortiOS v6.4.x
- FortiOS v6.2.x
- FortiOS v6.0.x

Fortinet agent support

FortiAuthenticator 6.3.0 supports the following Fortinet Agents:

- FortiClient v.5.x, v.6.x for Microsoft Windows (Single Sign-On Mobility Agent)
- FortiAuthenticator Agent for Microsoft Windows 2.6 and 3.7
- FortiAuthenticator Agent for Outlook Web Access 2.2
- FSSO DC Agent v.5.x
- FSSO TS Agent v.5.x

Other Agent versions may function correctly, but are not supported by Fortinet.

For details of which operating systems are supported by each agent, please see the install guides provided with the software.

Virtualization software support

FortiAuthenticator 6.3.0 supports:

- VMware ESXi / ESX 6/7
- Microsoft Hyper-V 2010, Hyper-V 2012 R2, and Hyper-V 2016
- Linux Kernel-based Virtual Machine (KVM) on Virtual Machine Manager and QEMU 2.5.0
- Xen Virtual Machine (for Xen HVM)
- Nutanix
- Amazon AWS
- Microsoft Azure
- Oracle OCI
- Alibaba Cloud

Support for HA in Active-Passive and Active-Active modes has not been confirmed on the FortiAuthenticator for Xen VM at the time of the release.

See FortiAuthenticator-VM on page 21 for more information.

Third-party RADIUS authentication

FortiAuthenticator uses standards based RADIUS for authentication and can deliver two-factor authentication via multiple methods for the greatest compatibility:

- RADIUS Challenge Response - Requires support by third party vendor.
- Token Passcode Appended - Supports any RADIUS compatible system.

FortiAuthenticator should therefore be compatible with any RADIUS capable authentication client / network access server (NAS).

FortiAuthenticator-VM

For information about FortiAuthenticator-VM deployments and system requirements, see the VM installation guide on the Fortinet Docs Library.

Resolved issues

The resolved issues listed below may not list every bug that has been corrected with this release. For inquiries about a particular bug, please visit the Fortinet Support website.

Bug ID	Description
544691	Remote LDAP admins have no certificate bindings.
666636	Wrong group attributes indicator in RADIUS policy response table for EAP-TLS.
676321	"Allowed shell commands" label in authorization rules is misleading.
677417	FSSO user/group filter import have misleading descriptions.
700837	SMS gateway HTTP/HTTPS - Inconsistent JSON object type used for phone-number attribute.
700957	User logon is not working with FSSOMA mobility agent.
652072	LDAP user password expired, user not prompted for RSA Token code (chained Token Authentication).
683298	Agent exception error occurred when OTP is delivered by SMS.
693210	Self-registration access via HTTP is allowed.
670811	Remote SAML user import from Azure AD issues.
673303	Fine-grained menu content has misaligned pointer in SSO/General.
467883	RDP Users prompted for credentials twice and failing the second time due to token reuse (if they do not wait).
685408	Restricted admin users have view of HA settings and can attempt to change them.
584589	Align logs on the left side instead of the center.
670827	FortiGate filtering stops any users sent to FortiGate even though users are member of group/container.
649999	SAML SSO Groups - not all are imported.
682170	When a user reports lost token and tries to switch to email token authentication, the email is never sent to the user with the token.
657522	SAML authentication fails when the AD display name contains a coma (,) and the user has an admin role.
645043	GUI does not show cert UPN.
685462	Longer IPv6 address cannot be set to the FortiAuthenticator interface.
689340	Secondary unit upgrade fails.
690250	Remote SAML user import from Azure AD - Not all users imported.
676311	FortiAuthenticator-VM hangs while quiescing the virtual machine.
694599	Certificate sync does not work from primary to LB peer/nodes.

Bug ID	Description
677935	Self-service portal does not work with remote LDAP user with administrator role profile, portal error: 403 Forbidden.
673151	Domain controller query status shows failed with successful queries.
680488	Gateway timed out error while creating a new user group.
666782	If local CA is selected for EAP and no EAP server certificate is present on FortiAuthenticator, radiusd keeps crashing after upgrading to 6.2.0.
632237	Remove device ID requirement when using Smart Connect.
693893	Display filter is not working correctly within the certificates section.
693920	Smart Connect user certificate generation fails due to certificate ID character limitation/autogeneration process.
701887	FortiAuthenticator Captive Portal is not providing correct redirection URL response to Apple iOS devices.
602707	Unable to add multiple alternate DNS names into certificate for user certificates.
677657	FortiAuthenticator timing out with known good SMTP server (port 587, no STARTTLS).
672750	When a user tries to access the Self-service portal, FortiAuthenticator gives the "Please enter correct credentials. Note password is case-sensitive" error randomly.
676225	RADIUS authentication with the remote RADIUS server stops working.
650215	FortiAuthenticator Windows Agent 3.0 - New RDP connection by the same user unable to finish due to blank login screen.
666880	GUI - Hide SNMP trap option for PSU monitoring for unsupported devices.
693207	LB Cluster fails to sync SAML configuration.
692994	Change in the default RADIUS authentication port makes the GUI inaccessible.
703275	Protection and warning when deleting a local CA (in the LB primary side).
673319	Admin cannot log in to approve the self-registration when group filters are set without admin user in a Guest Portal policy.
640048	FortiAuthenticator fails to load the license.
675195	Non-SMS RADIUS users unable to authenticate when the SMS gateway is down.
681102	Hitting the OpenLDAP size limit on FortiAuthenticator.
686551	Passwords of some local users on FortiAuthenticator are not expiring.
696064	LB sync deletes LB-created CA certificate but it still shows up in the UI list.
676595	Error creating RADIUS client (subnet) matching existing TACACS client (subnet).
543791	Users audit report does not update timestamps for LDAP users in the "last used" column.
697561	FortiAuthenticator 2000E missing power supply in the CLI and the GUI.

Bug ID	Description
672987	After upgrading FortiAuthenticator from 5.4 to 6.x Apple devices cannot load the FortiAuthenticator captive portal via the system pop-up only.
699562	License dashboard pane is not populating.
669079	HTTPS certificate chain is inconsistent/incorrect.
668337	Allowed hosts configuration through CLI not reflected in the GUI before reboot.
663582	Unable to disable maintenance mode in a HA cluster.
692726	Certificate expiry warning sends out an email everyday.
678195	TACACS+ service unstable after receiving many authentication attempts.
698736	FortiAuthenticator HA primary API PATCH method localuser-[ID] produces a 504 gateway timeout.
685872	Change in HTML for confirmation page after a successful logout from the guest portal "Logout Success Page".
666571	"Portal was not found in the session" when registering a guest with non-ASCII characters "Umlauts".
694682	Unable to import SSO filtering LDAP group from the eDirectory.
677228	Push notifications are not working for random users after upgrading to FortiAuthenticator 6.2.0 and 6.2.1.
675545	FortiAuthenticator is not sending optional Attribute-Value pairs.
688713	Duplicate remote LDAP users are not syncing.
697598	Mobile number formatting.
684202	Recover from corrupt FTM license configurations.
683266	FortiAuthenticator Windows agent- Push not working for some clients.
710223	FortiAuthenticator Agent: SMS token code not delivered for a user set with a blank password.
601603	CLI only supports configuring interfaces port1 - port4.
601520	Recurrent log message: Portal was not found in the session, redirecting back to the entry point.
660357	FSSO FortiGate IP filter ignored when the global group prefilter is enabled.
588346	An expired certificate is delivered toward WiFi authenticated users.
685330	SAML assertion request error in the date/time format.
671345	FortiAuthenticator Windows Agent prompts for token despite an incorrect password, and then does not prompt for user credentials again.
604924	SAML SSO/Proxy metadata download fails with "invalid_xml".
630041	FortiAuthenticator FSSO - TS Agent sessions stuck at zero after server reboot until FSSOTA service is restarted.
685368	SNMP access to the LB secondary fails.
705368	Transferring reassigned tokens triggered from the previous user sends email to the existing user.

Bug ID	Description
668916	Subdomain users can authenticate over FortiAuthenticator Agent installed on a workstation in the main domain without a token code.
673306	FortiAuthenticator Agent cannot initiate connection towards a secondary FortiAuthenticator for 2FA validation.
668045	On a LB node, a user certificate has the same SN in case of getting signed with synced local CA of standalone primary.
676199	Windows Agent 3.2 push notification accept fails on unlock and change password screens.
635893	Change password not working with Checkpoint VPN when 2FA is enabled.
615442	No Kerberos ticket requests (negotiate) on encrypted HTTPS traffic from FortiAuthenticator.
659402	CLI: Verify administrator password before reset default admin account.
674705	User Portal: Self-service policy cannot do MAC filtering.
666462	Lost messages from the serial port.
674673	GUI display of Power supply status is wrong.
659392	Ensure logs for push notification daemon are rotated.
693737	LB checksums not changing when local user passwords are updated.
693809	Rate limit REST API calls to authentication related endpoints.
708052	Old SAML IdP sessions not cleaned up by the expired session cleanup task.
694555	Unable to select admins from the MAC device page.
704794	Unable to delete social users.
683398	Remove "realm" field when FortiAuthenticator calls auth_post with arguments.
709726	No more pushd log after the old log is archived.
664328	HA LB status Users/User profiles keep going back to the out-of-sync status.
707708	Port over FortiOS changes to upgrade Windows Azure Agent for marketplace compatibility.
621047	rlm_facauth multi-thread support.
643334	If the MAC filter is enabled, but the configured radius attribute is missing from the packet, we deny the authentication.
605463	Update cert layout so that the subject column is usable and the "Renewable Before Expiry (days)" is sized appropriately for.
696457	Cloud initialization with CLI in config drive fails due to mandatory default password reset.
650889	XSS Vulnerability observed when editing a Replacement Message.
678484	Secure flag support in SSL/TLS HTTPS cookies to avoid cookie leaking.
690816	LDAP sync rule does not support switching between user types in admin case.

Bug ID	Description
673185	FortiAuthenticator 6.0.3 generates errors in the FSSO debug log showing max TS Agent number has been reached.
690625	Wildcard for the allowed host.
665256	REST API FTC push support.
699739	HA-cluster upgrade failed in the secondary side.
702199	DB level delete cascade is missing.
659251	Add "expires_in" field to /oauth/verify_token/ response.
690640	Remote sync rules only enable password recovery by email not by security questions.
704228	Support for SHA256 usage in SAML signature method.
687350	CSR issued by Windows cannot be signed by FortiAuthenticator 6.2.x.
604224	Add a way to expand FortiAuthenticator "data drive" file system if partition size increases.
708158	Support email/SMS 2FA for FTC.

Known issues

This section lists the known issues of this release, but is not a complete list. For inquires about a particular bug, please visit the Fortinet Support website.

Bug ID	Description
655350	The lockout policy does not appear to apply to username/token submissions to the /auth API endpoint.
606760	HA cluster and FortiAuthenticator GUI does not reflect correct HA status when the primary fails and the secondary becomes the new primary.
701758	Problem setting static IP address on a FortiAuthenticator-VM installed on a XenServer.
637028	SSL connection fails in case of the certificate expired issue is not explicit enough.
692839	Local cert for the GUI rejected despite SAN field.
697447	Octet/ASCII conversion for all RADIUS attribute-value pairs.
697969	SCEP errors displayed when there is no enrollment request from the client (FortiGate).
676985	Unable to import all FTK hardware tokens from the same purchase order; need to add them all manually.
526202	FortiAuthenticator does not check if the signature of CSR is valid.
669054	Unable to install FortiAuthenticator-VM-HV 6.2.0 on server 2012 R2.
709007	Error when importing a remote LDAP user.
646299	Nutanix AHV KVM based Hypervisor FortiAuthenticator upgrade from 6.0.4 to 6.1.x fail hangs on "Waiting for Database".
693151	Allow deletion of the expired user and the local service certificates.
638374	SCEP - Encryption/hash compatibility with clients.
676532	When FortiAuthenticator has a RADIUS client set as a subnet, RADIUS accounting disconnect messages are not sent.
632248	Unable to provide publisher details/assign code signing certificate to the Smart Connect profile.
592837	Sponsor accounts can add guest user accounts to non-guest groups.
680423	FortiAuthenticator Syslog FSSO injects speech mark (") around external user and group fields where none exist in the raw log.
710914	FortiAuthenticator limits various user fields to 30 characters, causing remote LDAP sync failures unexpectedly.
711940	Raid widget is showing wrong status.
709395	High CPU utilization by wmid process.
710931	Unable to import users by group membership from OpenLDAP when a group is added in an OU.

Bug ID	Description
694303	Connection between FortiAuthenticator and the Active directory crashes; customer cannot access the device.
631600	SCEP request by certmonger cannot be recognized by automatic enrollment request.
695110	Corp FortiAuthenticator SAML login failure to mantis after VPN is disconnected.
712263	HTTP services - CRL Downloads (/cert/crl) enabled, but we still get warning that HTTP access needs to be enabled.
680776	AP HA primary cannot change mgmt interface access configuration, and the option does not sync from the primary either.
709744	Script errors on logging in to Microsoft Teams using SAML (FortiAuthenticator as the idP).
685172	FortiAuthenticator A-P running in v6.2.1 does not sync with the secondary unit pre-authentication warning message, CLI and GUI timeout.
632239	Smart Connect should not require user to select the OS.
711675	Some users are not receiving push notification prompt on their mobile phone.
711676	Feature(monitors interface stability period) not visible on FortiAuthenticator HA cluster GUI.

Maximum values for hardware appliances

The following table lists the maximum number of configuration objects per FortiAuthenticator appliance that can be added to the configuration database for different FortiAuthenticator hardware models.

The maximum values in this document are the maximum configurable values and are not a commitment of performance.

Feature		Model					
		200E	400E	800F	1000D	2000E	3000E
System							
Network	Static Routes	50	50	50	50	50	50
Messages	SMTP Servers	20	20	20	20	20	20
	SMS Gateways	20	20	20	20	20	20
	SNMP Hosts	20	20	20	20	20	20
Administration	Syslog Servers	20	20	20	20	20	20
	User Uploaded Images	39	114	414	514	1014	2014
	Language Files	50	50	50	50	50	50
Realms		20	80	320	400	800	1600
Authentication							
General	Auth Clients (NAS)	166	666	2666	3333	6666	13333
	Users (Local + Remote)[1]	500	2000	8000	10000	20000	40000
	User RADIUS Attributes	1500	6000	24000	30000	60000	120000
	User Groups	50	200	800	1000	2000	4000
	Group RADIUS Attributes	150	150	2400	600	6000	12000
	FortiTokens	1000	4000	16000	20000	40000	80000
	FortiToken Mobile Licenses[2]	200	200	200	200	200	200
	LDAP Entries	1000	4000	16000	20000	40000	80000
	Device (MAC-based	2500	10000	40000	50000	100000	200000

Feature		Model					
		200E	400E	800F	1000D	2000E	3000E
	Auth.)						
	RADIUS Client Profiles	500	2000	8000	10000	20000	40000
	Remote LDAP Servers	20	80	320	400	800	1600
	Remote LDAP Users Sync Rule	50	200	800	1000	2000	4000
	Remote LDAP User Radius Attributes	1500	6000	24000	30000	60000	120000
FSSO & Dynamic Policies							
FSSO	FSSO Users	500	2000	8000	10000	20000	200000[3]
	FSSO Groups	250	1000	4000	5000	10000	20000
	Domain Controllers	10	20	80	100	200	400
	RADIUS Accounting SSO Clients	166	666	2666	3333	6666	13333
	FortiGate Services	50	200	800	1000	2000	4000
	FortiGate Group Filtering	250	1000	4000	5000	10000	20000
	FSSO Tier Nodes	5	20	80	100	200	400
	IP Filtering Rules	250	1000	4000	5000	10000	20000
Accounting Proxy	Sources	500	2000	8000	10000	20000	40000
	Destinations	25	100	400	500	1000	2000
	Rulesets	25	100	400	500	1000	2000
Certificates							
User Certificates	User Certificates	2500	10000	40000	50000	100000	200000
	Server Certificates	50	200	800	1000	2000	4000
Certificate Authorities	CA Certificates	10	10	50	50	50	50
	Trusted CA Certificates	200	200	200	200	200	200
	Certificate Revocation Lists	200	200	200	200	200	200
SCEP	Enrollment Requests	2500	10000	40000	50000	100000	200000

[1] Users includes both local and remote users.

[2] **FortiToken Mobile Licenses** refers to the licenses that can be applied to a FortiAuthenticator, not the number of FortiToken Mobile instances that can be managed. The total number is limited by the FortiToken metric.

[3] For the 3000E model, the total number of concurrent SSO users is set to a higher level to cater for large deployments.

Maximum values for VM

The following table lists the maximum number of configuration objects that can be added to the configuration database for different FortiAuthenticator virtual machine (VM) configurations.

The maximum values in this document are the maximum configurable values and are not a commitment of performance.

The FortiAuthenticator-VM is licensed based on the total number of users and licensed on a stacking basis. All installations must start with a FortiAuthenticator-VM Base license and users can be stacked with upgrade licenses in blocks of 100, 1,000, 10,000 and 100,000 users. Due to the dynamic nature of this licensing model, most other metrics are set relative to the number of licensed users. The **Calculating metric** column below shows how the feature size is calculated relative to the number of licensed users for example, on a 100 user FortiAuthenticator]-VM Base License, the number of auth clients (NAS devices) that can authenticate to the system is:

100 / 10 = 10

Where this relative system is not used e.g. for static routes, the **Calculating metric** is denoted by a "**-**". The supported figures are shown for both the base VM and a 5000 user licensed VM system by way of example.

Feature		Model			
		Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
System					
Network	Static Routes	2	50	50	50
Messaging	SMTP Servers	2	20	20	20
	SMS Gateways	2	20	20	20
	SNMP Hosts	2	20	20	20
Administration	Syslog Servers	2	20	20	20
	User Uploaded Images	19	Users / 20	19	250
	Language Files	5	50	50	50
Authentication					
General	Auth Clients (NAS)	3	Users / 3	33	1666
User Management	**Users** (Local + Remote)[1]	5	**********	100	5000

Feature		Model			
		Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
	User RADIUS Attributes	15	Users x 3	300	15000
	User Groups	3	Users / 10	10	500
	Group RADIUS Attributes	9	User groups x 3	30	1500
	FortiTokens	10	Users x 2	200	10000
	FortiToken Mobile Licenses (Stacked) [2]	3	200	200	200
	LDAP Entries	20	Users x 2	200	10000
	Device (MAC-based Auth.)	5	Users x 5	500	25000
	RADIUS Client Profiles	3	Users	100	5000
	Remote LDAP Servers	4	Users / 25	4	200
	Remote LDAP Users Sync Rule	1	Users / 10	10	500
	Remote LDAP User Radius Attributes	15	Users x 3	300	15000
FSSO & Dynamic Policies					

Feature		Model			
		Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
FSSO	FSSO Users	5	Users	100	5000
	FSSO Groups	3	Users / 2	50	2500
	Domain Controllers	3	Users / 100 (min=10)	10	50
	RADIUS Accounting SSO Clients	10	Users	100	5000
	FortiGate Services	2	Users / 10	10	500
	FortiGate Group Filtering	30	Users / 2	50	2500
	FSSO Tier Nodes	3	Users /100 (min=5)	5	50
	IP Filtering Rules	30	Users / 2	50	2500
Accounting Proxy	Sources	3	Users	100	5000
	Destinations	3	Users / 20	5	250
	Rulesets	3	Users / 20	5	250
Certificates					
User Certificates	User Certificates	5	Users x 5	500	25000
	Server Certificates	2	Users / 10	10	500
Certificate Authorities	CA Certificates	3	Users / 20	5	250
	Trusted CA Certificates	5	200	200	200
	Certificate Revocation Lists	5	200	200	200
SCEP	Enrollment Requests	5	Users x 5	2500	10000

[1] Users includes both local and remote users.

[2] **FortiToken Mobile Licenses** refers to the licenses that can be applied to a FortiAuthenticator, not the number of FortiToken Mobile instances that can be managed. The total number is limited by the FortiToken metric.

www.fortinet.com